RouteFinder™ VPN

Internet Security Appliance

RF760/660/600VPN

Internet Security Appliance

Quick Start Guide

MultiTech® Systems

Quick Start Guide
RouteFinder VPN RF760/660/600VPN
82013762L, Revision C

Copyright

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.
Copyright © 2004-5, by Multi-Tech Systems, Inc.
Multi-Tech Systems, Inc. makes no representations or warranty with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.
Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Record of Revisions

Revision	Date	Description
A	01/15/04	Initial release for RF760VPN. Include RF600VPN and RF660VPN to create a combo guide.
B	10/26/04 & 01/25/05	New software – version 3.20 and New software – version 3.21. POP3 Proxy added to the software.
C	12/02/05	New software – version 3.25. New Hardware: compact flash.

Patents

This device is covered by one or more of the following U.S. Patent Numbers: 6,219,708; 5,301,274; 5,309,562; 5,355,365; 5,355,653; 5,452,289; 5,453.986.
The modem is covered by one or more of the following U.S. Patent Numbers: 6,031,867; 6,012,113; 6,009,082; 5,905,794; 5,864,560; 5,815,567; 5,815,503; 5,812,534; 5,809,068; 5,790,532; 5,764,628; 5,764,627; 5,754,589; D394,250; 5,724,356; 5,673,268; 5,673,257; 5,644,594; 5,628,030; 5,619,508; 5,617,423; 5,600,649; 5,592,586; 5,577,041; 5,574,725; D374,222; 5,559,793; 5,546,448; 5,546,395; 5,535,204; 5,500,859; 5,471,470; 5,463,616; 5,453,986; 5,452,289; 5,450,425; D361,764; D355,658; D355,653; D353,598; D353,144; 5,355,365; 5,309,562; 5,301,274 Other Patents Pending

Copyrights and Trademarks

Trademarks of Multi-Tech Systems, Inc.: Multi-Tech, the Multi-Tech logo and RouteFinder.
Windows is a registered trademark of Microsoft Corporation in the United States and other countries. Kaspersky Anti-Virus engine copyrighted by Kaspersky Labs. GNU General Public License copyrighted by Free Software Foundation, Inc. Surfcontrol is the registered product of Surfcontrol PLC. All products or technologies are the trademarks or registered trademarks of their respective holders.

Warranty, Repairs & Service, Licenses

The following statements and policies are printed in the RouteFinder User Guide.
They are also available on the RouteFinder CD and the Multi-Tech Web site at www.multitech.com.

- Multi-Tech Systems, Inc. Warranty Statement
- Multi-Tech Systems, Inc. Repairs and Service Policy
- Multi-Tech Systems, Inc End User License
- GNU General Public License
- SurfControl URL Filtering End-User Terms
- Kasperkey Standard End User License Agreement.

Technical Support

Country	By Email	By Phone
France:	support@multitech.fr	(33) 1-64 61 09 81
India:	support@multitechindia.com	91 (124) 6340778
U.K.:	support@multitech.co.uk	(44) 118 959 7774
U.S. and Canada:	support@multitech.com	(800) 972-2439
Rest of the World:	support@multitech.com	(763) 717-5863

World Headquarters

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(763) 785-3500 or (800) 328-9717
Fax 763-785-9874
Internet Address: http://www.multitech.com

Contents

Chapter 1 – Introduction **5**
The RouteFinder and Its Documentation 5
Other References 5
Safety Warnings 5
Safety Recommendations for Rack Installations 6
Ship Kit Contents 6
License Keys 6
Typical Applications 7
Chapter 2 – Installation **8**
Installation – Planning the Network 8
Establishing an Address Table 8
Cabling Procedure 9
Setting up a Workstation and Starting the RouteFinder VPN 10
Navigating Through the Screens 12
Initial Web Administration Steps 14
Chapter 3 – Using the Wizard Setup **14**
Initial Configuration Using the Wizard Setup 14
Using the Setup Wizard 16
Chapter 4 – Configuration Examples **17**
Example 1: LAN-to-LAN VPN (Branch Office) 17
Example 2: Remote Client-to-LAN VPN Configuration 22
Example 3: Remote Client-to-LAN Configuration Using DNAT and Aliasing 23
Example 4: Client-to-LAN Configuration Using PPTP Tunneling 24
Chapter 5 - URL Categorization **25**

Chapter 1 – Introduction

The RouteFinder and Its Documentation

The RouteFinder VPN is both a Virtual Private Network (VPN) and a firewall. It also offers an optional email antivirus protection subscription.

Using the RouteFinder VPN is a cost-effective, manageable way for small to medium businesses to add a remote user VPN, a Branch Office VPN, and/or Firewall Security applications to their networks.

This Quick Start Guide is intended to provide the experienced system administrator the information needed to quickly get the RouteFinder VPN up and running. A User Guide with more detailed information is provided on the RouteFinder VPN CD.

Other References

In addition to the User Guide, the following Reference Guides are available on the CD as well as the Multi-Tech Web site at www.multitech.com:

1. The RouteFinder configured with DNAT and aliases.
2. Setting up a PPTP server and a PPTP remote client.
3. The VPN tunnel configured for manual mode example and IPSec pass-through in manual mode example.
4. A guide for the add-on product, IPSec SSH client.
5. Hard-Disk Drive Recovery.

Safety Warnings

Lithium Battery Caution

Danger of explosion if battery is incorrectly replaced. A lithium battery on the RouteFinder VPN PC board provides backup power for the time-keeping capability. The battery has an estimated life expectancy of ten years. When it starts to weaken, the date and time may be incorrect. If the battery fails, send the board back to Multi-Tech for battery replacement.

Ethernet Ports Caution

The Ethernet ports are not designed to be connected to a Public Telecommunication Network.

Software Recovery CD Warning

Do not use the Software Recovery CD for any purpose except for re-installing software onto the RouteFinder VPN hard drive.

Telecom Warnings for Modem Operation

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in a wet location unless the jack is specifically designed for wet locations.
- This product is to be used with UL and cUL listed computers.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Avoid using a telephone during an electrical storm. There may be a remote risk of electrical shock from lightening.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- To reduce the risk of fire, use only No. 26 AWG or larger Telecommunications line cord.

Safety Recommendations for Rack Installations

- Ensure proper installation of the RF760/660VPN in a closed or multi-unit enclosure by following the recommended installation as defined by the enclosure manufacturer.
- IMPORTANT: Do not place the RF760/660VPN directly on top of other equipment or place other equipment directly on top of the RF760/660VPN.
- If installing the RF760/660VPN in a closed or multi-unit enclosure, ensure adequate airflow within the rack so that the maximum recommended ambient temperature is not exceeded.
- Ensure that the RF760/660VPN is properly connected to earth ground via a grounded power cord. If a power strip is used, ensure that the power strip provides adequate grounding of the attached apparatus.
- Ensure that the main supply circuit is capable of handling the load of the RF760/660VPN. Refer to the power label on the equipment for load requirements.
- Maximum ambient temperature for the RF760/660VPN is 50 degrees Celsius (120° F).
- This equipment should only be installed by properly qualified service personnel.
- Only connect like circuits. In other words, connect SELV (Secondary Extra Low Voltage) circuits to SELV circuits and TN (Telecommunications Network) circuits to TN circuits.

Ship Kit Contents

The RouteFinder VPN is shipped with the following:

- One Multi-Tech Systems, Inc. RouteFinder VPN
- One Power Cord
- One printed Quick Start Guide
- One external Power Supply for the RF600VPN.
  Note: The power supply for the RF760VPN and RF660VPN is internal.
- Two Rack Mounting Brackets and four mounting screws.
  Note: See the User Guide on the documentation CD for rackmounting directions.
- One RouteFinder VPN documentation CD which contains documentation, license agreements, Adobe Acrobat Reader, and License keys.
- One RouteFinder VPN Software Recovery CD.

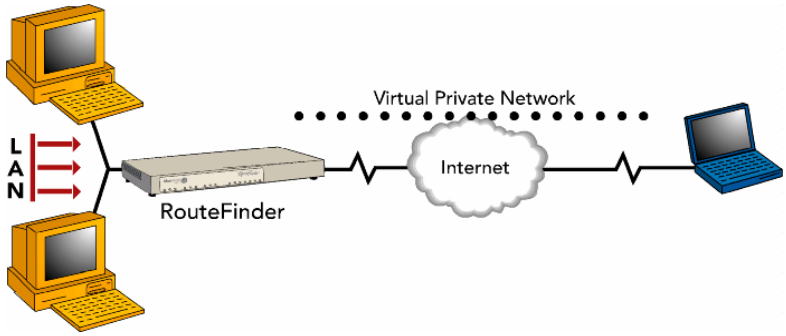
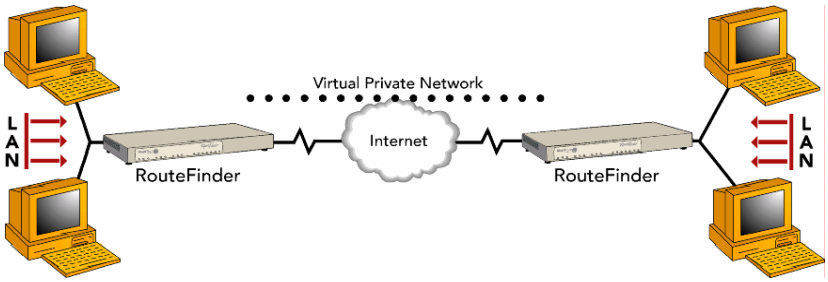
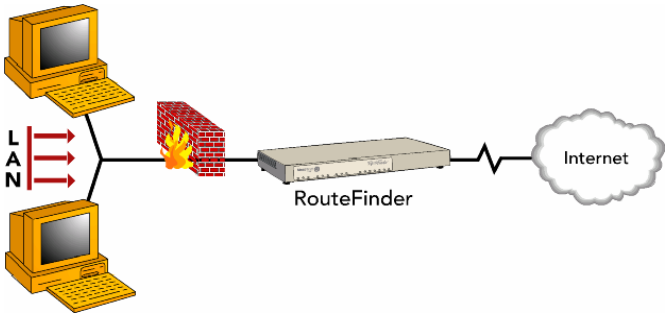
Warning: Do not use the Software Recovery CD for any purpose except for re-installing software onto the RouteFinder VPN hard drive.

Note: If any of these items are missing, contact Multi-Tech Systems or your dealer or distributor. Inspect the contents for signs of any shipping damage. If damage is observed, do not power up the RouteFinder VPN; contact Technical Support at Multi-Tech Systems, Inc. for advice.

License Keys

Where to find the License Key Number Label: The VPN License Key number and the URL License Key number are printed on labels and are placed on the bottom of the RouteFinder chassis, on the hard drive inside the chassis, and on the front cover of the Quick Start Guide. These license numbers will have to be entered into the RouteFinder configuration setup using the RouteFinder built-in software.

Typical Applications

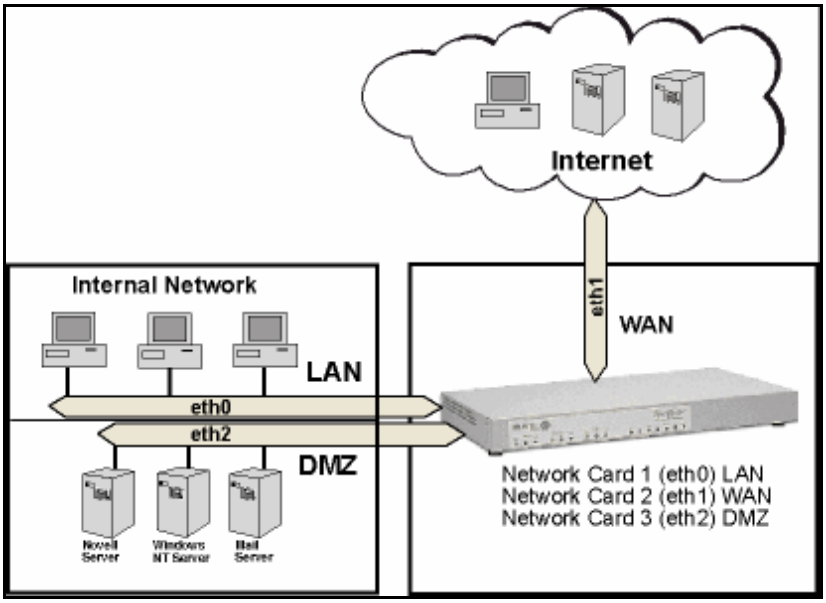
Remote User VPN. The client-to-LAN VPN application replaces traditional dial-in remote access by allowing a remote user to connect to the corporate LAN through a secure tunnel over the Internet. The advantage is that a remote user can make a local call to an Internet Service Provider, without sacrificing the company's security, as opposed to a long distance call to the corporate remote access server.	
Branch Office VPN. The LAN-to-LAN VPN application sends network traffic over the branch office Internet connection instead of relying on dedicated leased line connections. This can save thousands of dollars in line costs and reduce overall hardware and management expenses.	
Firewall Security. As businesses shift from dial-up or leased line connections to always-on broadband Internet connections, the network becomes more vulnerable to Internet hackers. The RouteFinder VPN provides a full-featured firewall based on Stateful Packet Inspection technology and NAT protocol to provide security from intruders attempting to access the office LAN.	

Chapter 2 – Installation

Installation – Planning the Network

Before you begin the installation process, you should plan your network and decide which computer is to have access to which services. This simplifies configuration and saves you a lot of time that you would otherwise need for corrections and adjustments.

RouteFinder VPN Connection between Your Internal Network and the External Network



Establishing an Address Table

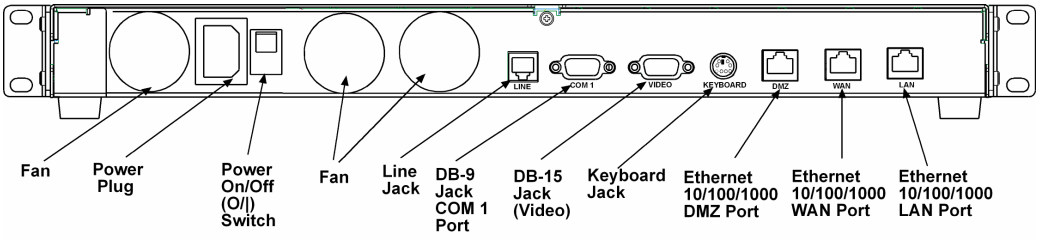
Enter your configuration information into the appropriate field of the Address Table below. You can use this table to keep track of your specific RouteFinder VPN and network information (e.g., the IP address used, email lists, etc.) and keep for future reference.

	IP Address	Net Mask	Default Gateway
Network Card connected to the internal network (LAN on eth0)	___.___.___.___	___.___.___.___	
Network Card connected to the external network (WAN on eth1)	___.___.___.___	___.___.___.___	___.___.___.___
Network Card connected to the DMZ (eth2)	___.___.___.___	___.___.___.___	

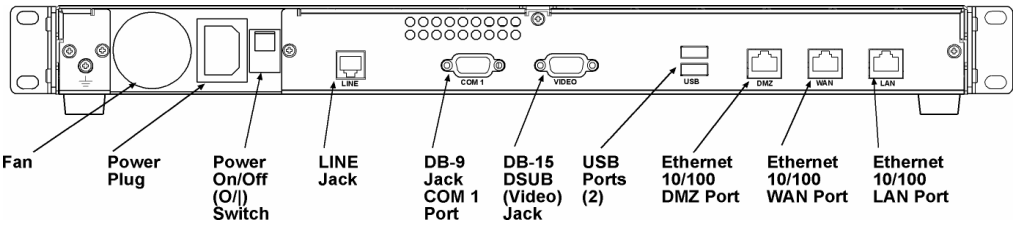
Cabling Procedure

Cabling your RouteFinder VPN involves making the proper Power, DMZ, WAN and LAN connections as illustrated and described below.

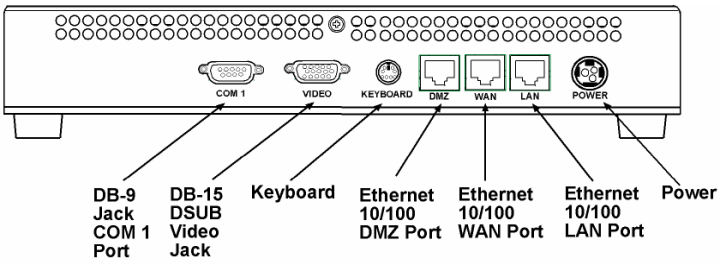
RF760VPN



RF660VPN



RF600VPN



1. Using an RJ-45 Ethernet cable, connect the DMZ RJ-45 jack to the DMZ device or network (Optional – for example, a Voice over IP gateway).
2. Using an RJ-45 Ethernet cable, connect the WAN RJ-45 jack to the device for the external network.
3. Using an RJ-45 Ethernet cable, connect the LAN RJ-45 jack to the internal network switch or hub.

   Note: Use a cross-over Ethernet cable if connecting to a single device.
4. With the RF760 or RF660 RouteFinder VPN Power switch in the off (O) position and using the supplied power cord, plug one end into the RouteFinder VPN connect power plug and the other end into a live power outlet.

   Note: The status LED blinks continuously after power-up.
5. Wait for the RouteFinder VPN to beep five times, indicating that it is ready to be configured with a Web browser.

Shutdown Caution

Never switch off the RouteFinder VPN Power until after you have performed the **Shutdown** process. If the RouteFinder VPN is not properly shut down before switching off Power, the next startup may take a little longer, or in the worst case, data could be lost.

Setting up a Workstation and Starting the RouteFinder VPN

This section of the Quick Start Guide covers the steps for setting up a workstation that is connected to the RouteFinder VPN, starting up the RouteFinder VPN, opening the RouteFinder VPN Web Management program, performing the time zone setup, and using the Menu bar to navigate through the Web Management software screens.

Connections

1. Connect a workstation to the RouteFinder's **LAN** port via Ethernet. Connections are described on the previous page.

   Note: If not using a hub, use a cross-over cable to connect a PC NIC to the RouteFinder's Ethernet 10/100 LAN Port.
2. Set the workstation IP address to **192.168.2.x** subnet.
3. Obtain an Internet Public IP address so it can be assigned to the WAN port.
4. Connect to the Internet at the RouteFinder **WAN** port.

Power Up

5. Turn on power to the RouteFinder VPN. After several minutes, you will hear 5 beeps signifying the software has fully booted.

   Note: If you hear a continuous beep or no beep, cycle RouteFinder VPN power, connect an external monitor and check the hard drive.

Open a Web Browser

6. Bring up a Web browser on the workstation. Type the default Gateway address: **https://192.168.2.1** and press the **Enter** key.

IMPORTANT: Be sure to type **https** (**http** will not work).

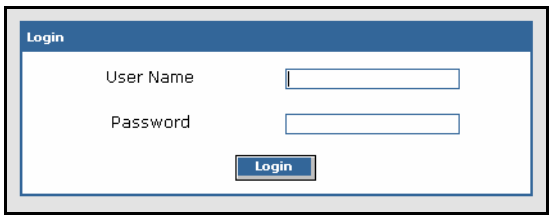
Note: Make sure your PC's IP address is in the same network as the router's IP address. **WINIPCFG** and **IPCONFIG** are tools for finding a computer's default gateway and MAC addresses. In Windows 98/ME you can type **WINIPCFG**. In Windows 2000/NT/ME/XP, you can type **IPCONFIG**.

7. In some environments, one or more Security Alert screen(s) may display. At the initial **Security Alert** screen, click **Yes** and follow any additional on-screen prompts.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate matches the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

Login

8. The **Login** screen is displayed.



- Type the default User name: **admin** (all lower-case)
- Tab to the Password field and type the default password: **admin** (all lower-case).
- Click the **Login** button.

Note: The **User name** and **Password** entries are case-sensitive (both must be typed in lower-case). The password can be up to 12 characters. Later, you will want to change the password from the default (**admin**) to something else. If Windows displays the **AutoComplete** screen, you may want to click **No** to tell Windows OS to not remember the password for security reasons.

Password Caution: Use a safe password! Your first name spelled backwards is not a sufficiently safe password; a password such as xfT35$4 is better.

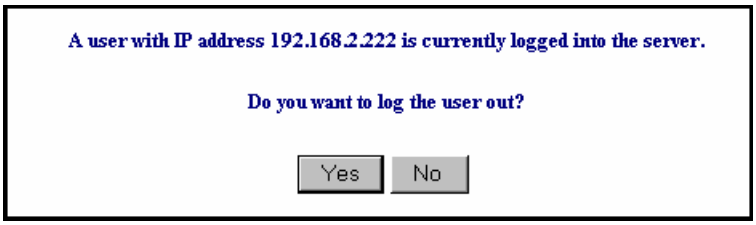
It is recommended that you change the default password. Create your own password.

9. If someone else is already logged onto the RouteFinder VPN or you were logged in recently, the following message displays.

Do you want to log the user out?

Click **Yes**.

If you click **No**, you are returned to the Login screen.



Web Management Software Opens

The Web Management **Home** screen is displayed. Web Management software is factory-installed on your RouteFinder.

(This is a view of the top part of the Home screen.)

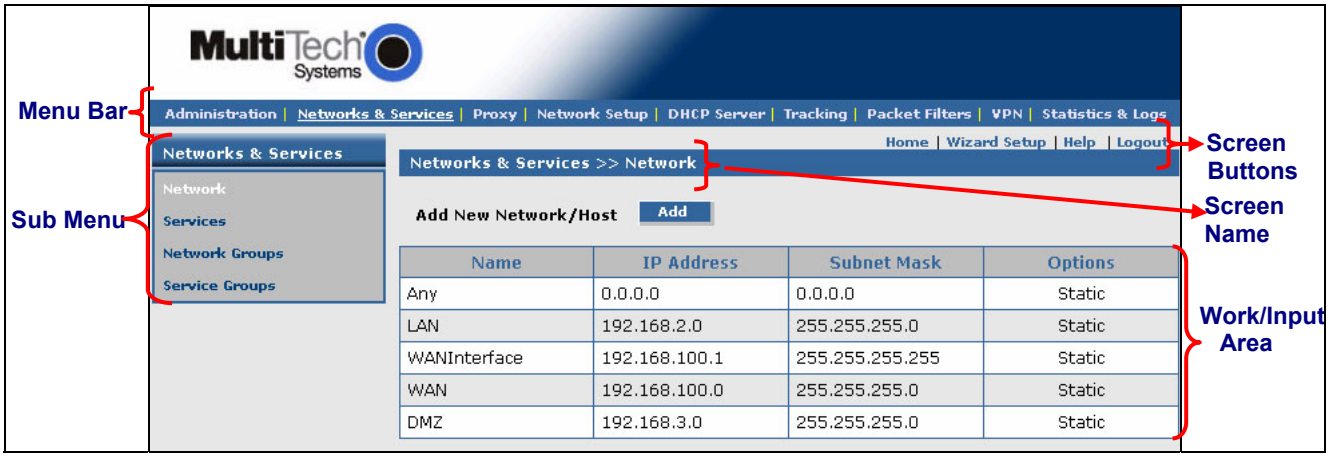
MultiTech Systems
Administration | Networks & Services | Proxy | Network Setup | DHCP Server | Tracking | Packet Filters | VPN | Statistics & Logs
Home | Wizard Setup | Help | Logout
Home
Home Page
Help
Home >> Home Page
RouteFinder Internet Security Appliance

(This is a view of the Multi-Tech Systems, Inc. informational part of the Home screen.)

Navigating Through the Screens

Before using the software, you may find the following information about navigating the screens and the structuring of the menus helpful.

The Web Management Screen



RouteFinder Menu Bar

Menu Selections

Administration	Setup system parameters, Administrative Access, User Authentication; enter licenses and certificates, etc. See entire list of functions on next page.
Networks & Services	Define network, services, and groups to make them available to be used by other functions such as allowed networks, packet filters, VPN, and proxies.
Proxy	Set up proxies.
Network Setup	Set up the LAN, WAN, and DMZ Ethernet ports; PPP modem link, etc.
DHCP Server	Configure the DHCP server settings.
Tracking	Set up tracking of all packets through the network ports in the RouteFinder VPN, set up automatic download and upgrade of packages from a specified Update server, set up import/export backup configurations.
Packet Filters	Define filter rules and ICMP rules.
VPN	Virtual Private Network. Set up a secure communication tunnel to specific Internet systems.
Statistics & Logs	View and download all the statistics and log files maintained by your system.

Screen Buttons

Home	The main screen.
Wizard Setup	Change passwords and quickly set up your RouteFinder VPN with the basic configuration that will set it up as a firewall.
Help	Describes what to do on each screen.
Logout	Logout and return to the login screen.

Sub-Menu

Each item on the Menu Bar has its own sub-menu, which displays on the left side of the screen.

When you click one of the Menu Bar buttons, the screen that displays is the first sub-menu option. You can choose other sub-menu screens by clicking the screen name in the sub-menu.

This is an example of the **Administration** sub-menu. It displays when **Administration** is clicked on the Menu Bar.

Menus and Sub-Menus

Administration	Networks & Services	Proxy	Network Setup	DHCP Server
System Setup SSH SNTP Client Administrative Access Site Certificate License Key Intrusion Detection Tools System Scheduler Factory Defaults User Authentication Local Users Radius & SAM Restart Shutdown	Network Services Network Groups Service Groups	HTTP Proxy Custom Filters SMTP Proxy SMTP SPAM Filtering POP3 Proxy POP3 SPAM Filtering SOCKS Proxy DNS Proxy	Interface PPP PPPoE DHCP Client Dynamic DNS Routes Masquerading SNAT DNAT	Subnet Settings Fixed Addresses

Tracking	Packet Filters	VPN	Statistics & Logs
Accounting Update Services Backup Version Control	Packet Filter Rules ICMP Advanced Enable/Disable Log	IPSec X.509 Certificates IPSec Bridging PPTP	Uptime Hardware Networks Interfaces SMTP Proxy Accounting Self Monitor IPSec PPTP Packet Filter Port Scans View Logs HTTP Access DHCP SMTP Virus Quarantine POP3 Virus Quarantine SMTP Spam Quarantine Administrative Authentication Log

Chapter 3 – Configuration

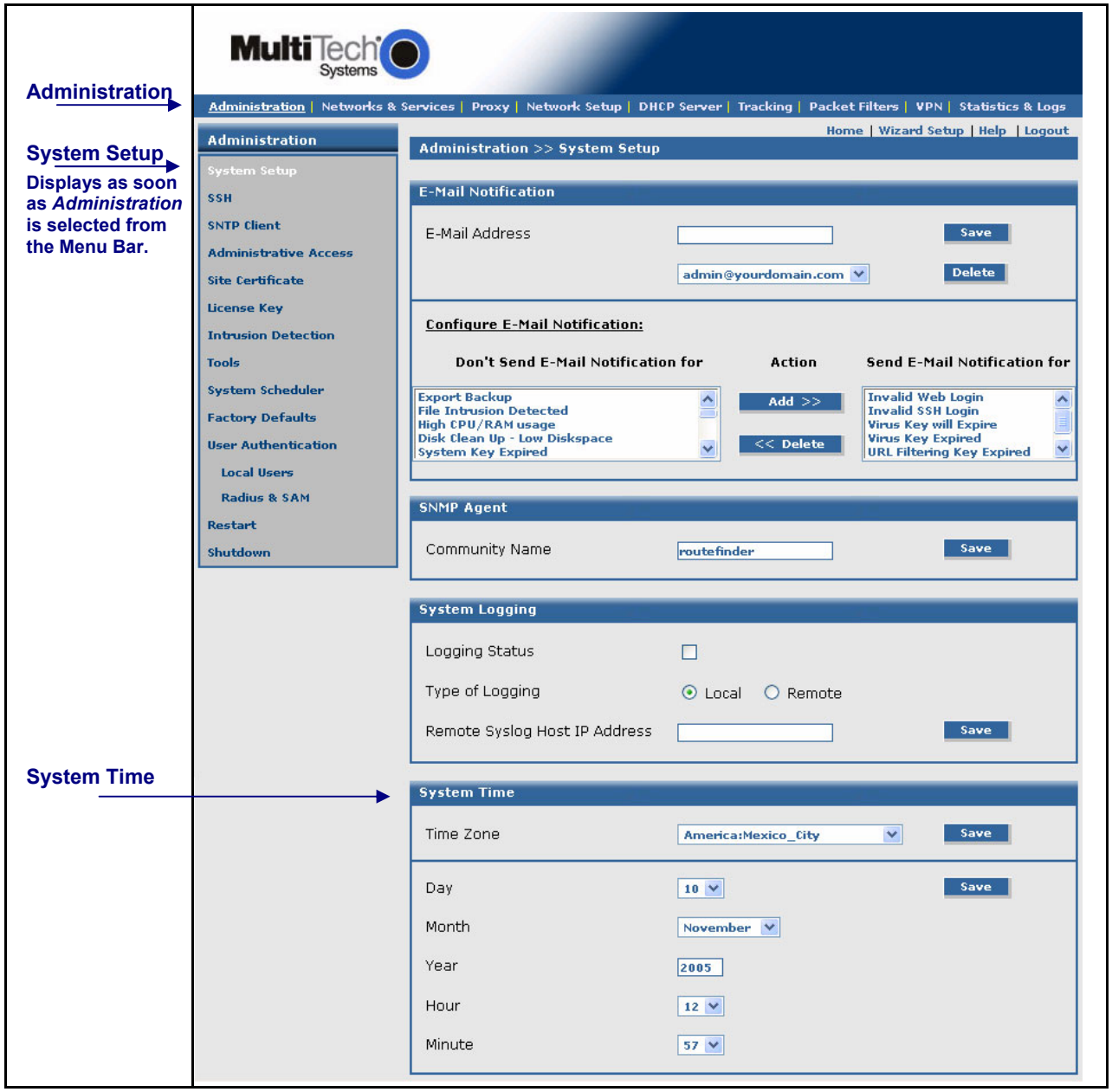
Initial Configuration Step

Set Up Your Time Zone

Click **Administration** on the Menu Bar. The **System Setup** screen displays.

Set the following:

- Set **System Time** by selecting your **Time Zone**
- Set the current **Day**, **Month**, **Year**, **Hour**, and **Minute**

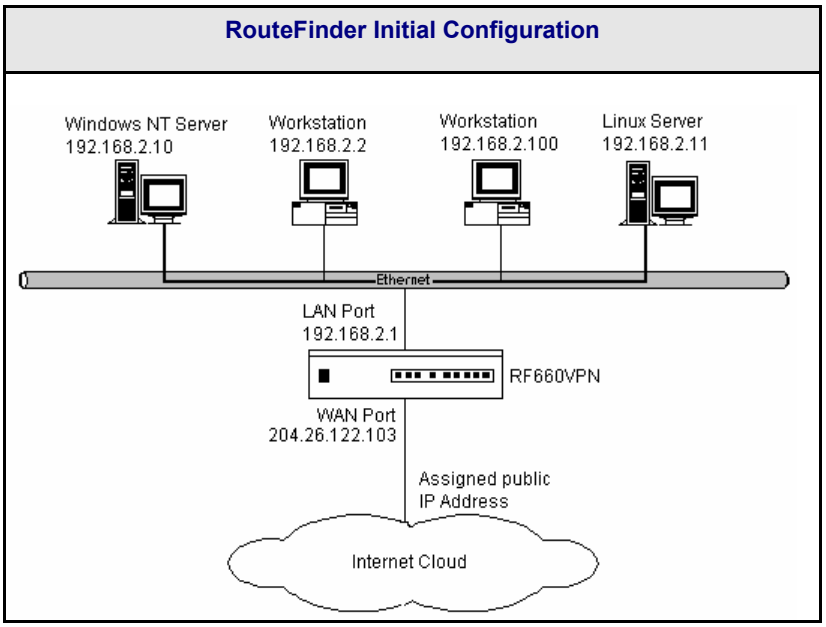


Second Configuration Step – Using the Wizard Setup

Using the Wizard Setup is a quick way to enter the basic configuration parameters to allow communication between the LAN's workstation(s) and the Internet as shown in the example below.

Important Note: An initial configuration must be completed for each type of RouteFinder functions: firewall configuration, LAN-to-LAN configuration, a LAN-to-Remote Client configuration.

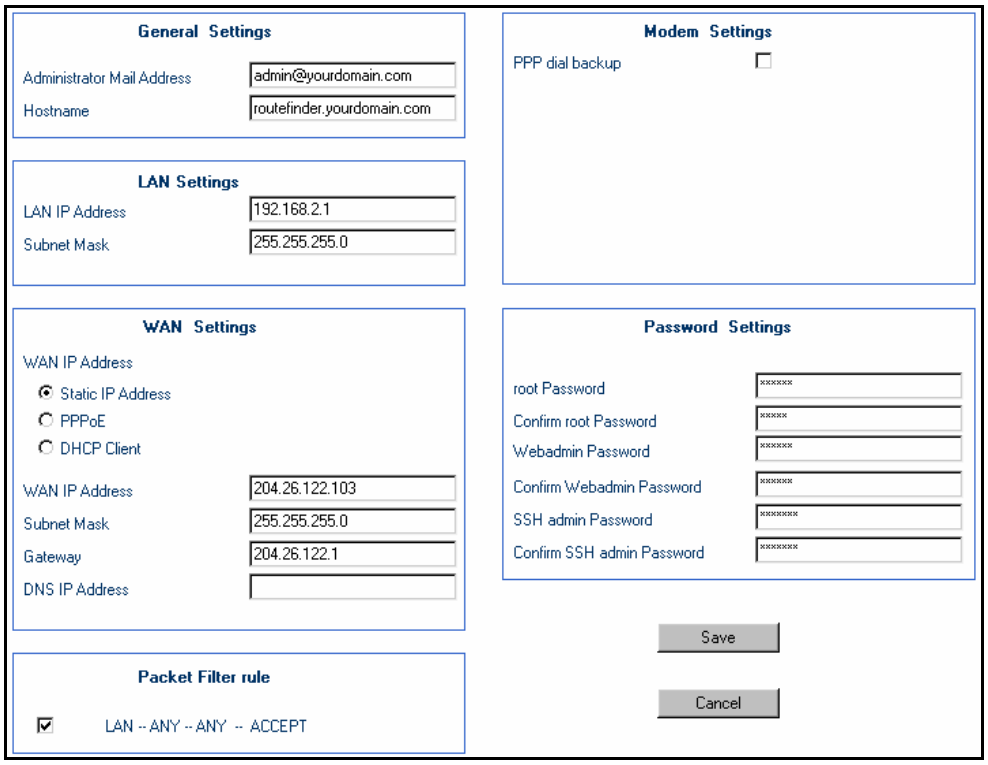
Note about License Agreements: It is suggested that you read the legal information and license agreements before beginning the configuration. This information can be found in the RouteFinder User Guide on the RouteFinder CD.



The addresses used in this example are entered through the Wizard Setup. See the screen example on the next page.

The Wizard Setup Screen

Click on the **Wizard Setup** button located under the Menu Bar. The following screen displays.



1. Enter your **Administrator Email Address** (can be anything).
   Example: admin@yourdomain.com
2. Enter your **Hostname** for the RouteFinder VPN (can be anything).
   Example: RouteFinder VPN.domainname.com
3. **LAN IP Address** and **Subnet Mask** default into the fields. These should be acceptable for your site.
4. Enter the **WAN IP Address**. This is the PUBLIC STATIC IP address.
   Set this option based on information provided by your ISP. Example: 204.26.122.103
5. Change the **Gateway IP address**; this is the IP address of the router that connects to the Internet. Example: 204.26.122.1
6. Place a checkmark in the **Packet Filter Rule LAN-ANY-ANY-ALLOW** box to enable the rule.
7. Change **Password Settings** as appropriate for your network. It is highly recommended that you change all default passwords. Do not leave them at the defaults for security reasons.
8. Click **Save** to save the settings you just entered.
9. The following message displays. Click **OK** to close the message box and save your changes.

   Click OK to save the changes. Please be patient. Wizard Setup will take a few minutes to implement the changes. Do not close the Browser.

10. One more message displays. Note that saving your settings will take 1-2 minutes.

    Please do not close the browser. Server is saving the values. After a few minutes you will be redirected to the new IP address. If you are not redirected, change the address in the location bar to 192.168.2.1.

11. Test your workstation to see that it can access the Internet. If a connection is established, then the settings have been entered correctly.

Your Basic Configuration Is Now Complete.

Chapter 4 – Configuration Examples

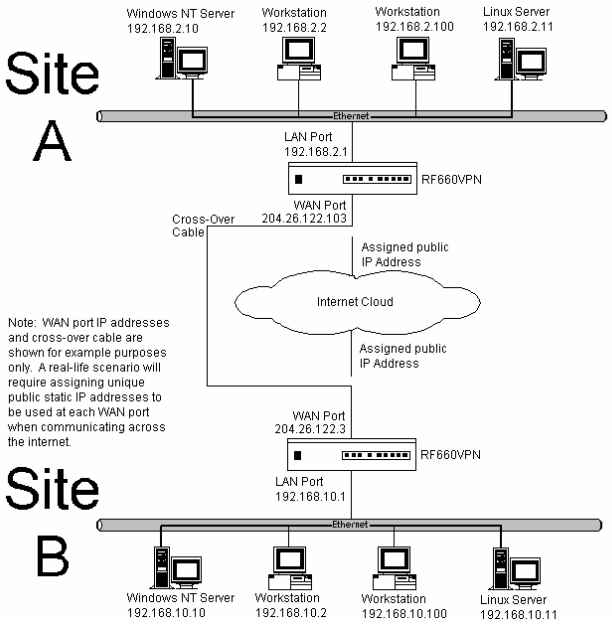
These examples show how to configure the RouteFinder using the entire Web Management software program. The Wizard Setup utility provides a basic connection, while the Web Management software allows you to configure firewall features, VPN features, management features, and other options (see the menu outline in Chapter 2).

Example 1 – LAN-to-LAN VPN (Branch Office)

The setup for a LAN-to-LAN VPN (branch office) requires two RF660VPNs - one in the home office and one in the remote branch office. It requires additional parameters beyond the Wizard Setup to be entered; these are listed in the table below. For the RouteFinder VPN in remote branch office follow the same procedures as the home office procedures; just use different IP addresses. The addresses and parameters in this example are used throughout this chapter as a point of reference for you.

Site A - Static IP Addresses. Input these parameters using the RF660VPN in the home office.

1. Domain name = site-A.com
2. Public Class C = 204.26.122.x
3. Networks & Services > Network
   LAN: 192.168.2.0 – 255.255.255.0
   RemoteLAN: 192.168.10.0 – 255.255.255.0
   RemoteWAN_IP: 204.26.122.3 – 255.255.255.255
4. Network Setup > Interface
   Default gateway = 204.26.122.1
   Host name = RF660VPN.site-A.com
   Eth0 = LAN, 192,168.2.1, 255.255.255.0
   Eth1 = WAN, 204.26.122.103, 255.255.255.0
   Eth2 = DMZ (don't care)
5. Packet Filters > Packet Filter Rules
   LAN – Any – Any – Accept
   RemoteLAN – Any – Any – Accept
6. VPN > IPSec
   Checkmark and Save VPN Status
   Add an IKE connection:
   - Connection name = SiteA
   - Checkmark Perfect Forward Secrecy
   - Authentication Method = Secret
   - Enter secret key (must be same on both sides)
   - Select Encryption = 3DES
   - Local WAN IP = WAN
   - Local LAN = LAN
   - Remote Gateway IP = RemoteWAN_IP
   - Remote LAN = RemoteLAN
   - Disable UID


Site A
Windows NT Server 192.168.2.10
Workstation 192.168.2.2
Workstation 192.168.2.100
Linux Server 192.168.2.11
Ethernet
LAN Port 192.168.2.1
RF660VPN
WAN Port 204.26.122.103
Cross-Over Cable
Assigned public IP Address
Internet Cloud
Assigned public IP Address
Note: WAN port IP addresses and cross-over cable are shown for example purposes only. A real-life scenario will require assigning unique public static IP addresses to be used at each WAN port when communicating across the internet.
WAN Port 204.26.122.3
RF660VPN
LAN Port 192.168.10.1
Site B
Ethernet
Windows NT Server 192.168.10.10
Workstation 192.168.10.2
Workstation 192.168.10.100
Linux Server 192.168.10.11

Site B - StaticIP Addresses. Input these parameters using the RF660VPN in the branch office.

1. Domain name = site-B.com
2. Public Class C = 204.26.122.x
3. Networks & Services > Network
   LAN: 192.168.10.0 – 255.255.255.0
   RemoteLAN: 192.168.2.0 – 255.255.255.0
   RemoteWAN_IP: 204.26.122.103 – 255.255.255.255
4. Network Setup > Interface
   Default gateway = 204.26.122.1
   Host name = RF660VPN.site-B.com
   Eth0 = LAN, 192.168.10.1, 255.255.255.0
   Eth1 = WAN, 204.26.122.3, 255.255.255.0
   Eth2 = DMZ (don't care)
5. Packet Filters > Packet Filter Rules
   LAN – Any – Any – Accept
   RemoteLAN – Any – Any – Accept

Site B - Static IP Addresses (continued)

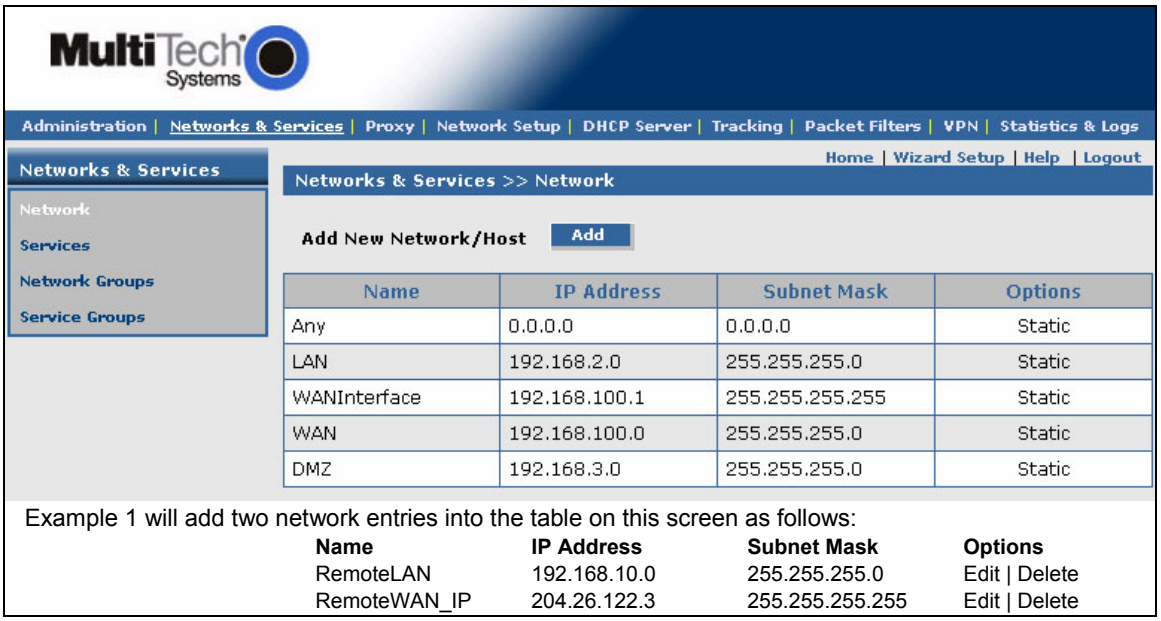
6. VPN > IPSec
   Checkmark and Save VPN Status
   Add an IKE connection:
   - Connection name = SiteB
   - Checkmark Perfect Forward Secrecy
   - Authentication Method = Secret
   - Enter secret key (must be the same on both sides)
   - Select Encryption = 3DES
   - Local WAN IP = WAN
   - Local LAN = LAN
   - Remote Gateway IP = RemoteWAN_IP
   - Remote LAN = RemoteLAN
   - Disable UID

Setup Networks & Services

Site A Configuration on the RouteFinder VPN in the Home Office

To configure your RouteFinder VPN in the home office in preparation for connection to a remote branch office, click the **Networks & Services** button on the Menu bar, and then select **Network**. Set the following:

1. Add a network for the remote LAN port (private LAN on eth0 at the branch office). Enter the following:
   - Name = RemoteLAN
   - IP address = 192.168.10.0
   - Subnet mask = 255.255.255.0
2. Add a network for the remote WAN port (public WAN on eth1 at the branch office). Enter the following:
   - Name = RemoteWAN_IP
   - IP address = 204.26.122.3
   - Subnet mask = 255.255.255.255



Example 1 will add two network entries into the table on this screen as follows:

Name	IP Address	Subnet Mask	Options
RemoteLAN	192.168.10.0	255.255.255.0	Edit | Delete
RemoteWAN_IP	204.26.122.3	255.255.255.255	Edit | Delete

Notes:

- **Default Entries**
  The first four entries on this screen are default entries and cannot be changed.

- **Network Data Displays on Other Screens**
  Networks added using the **Add Network/Host** on this screen will display in the *Remote Gateway IP* and *Remote LAN* dropdown boxes on the **VPN > IPSec > IKE** screen.

Set Packet Filters

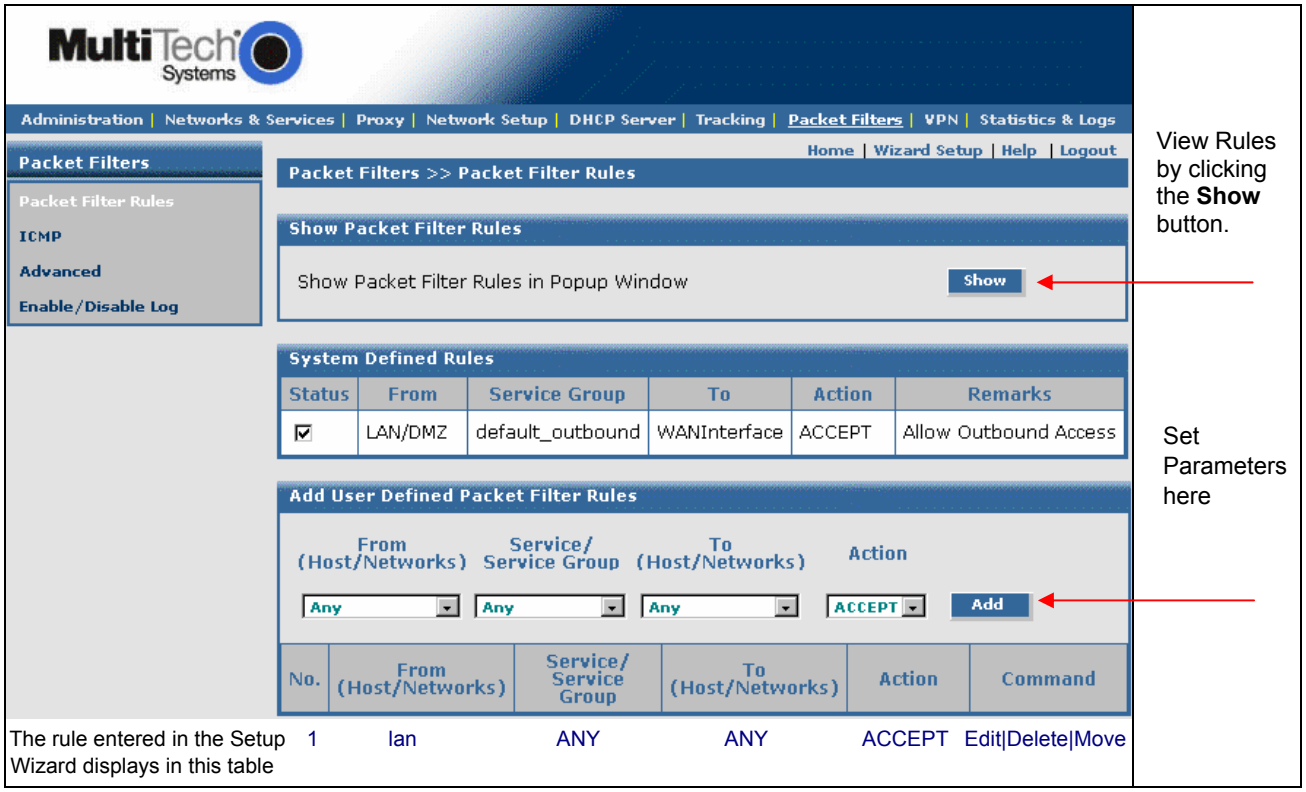
Site A Configuration: RouteFinder VPN in the Home Office

Establish remote access filtering: click on **Packet Filters > Packet Filter Rules**.

1. For the **Remote LAN** at the branch office to access the RouteFinder's LAN, select the following parameters for the Remote LAN rule:

   RemoteLAN – Any – Any – Accept

   Note: The rule **LAN – Any – Any – Accept**, which displays at the bottom of the screen, was created when you performed your initial setup using the Setup Wizard.

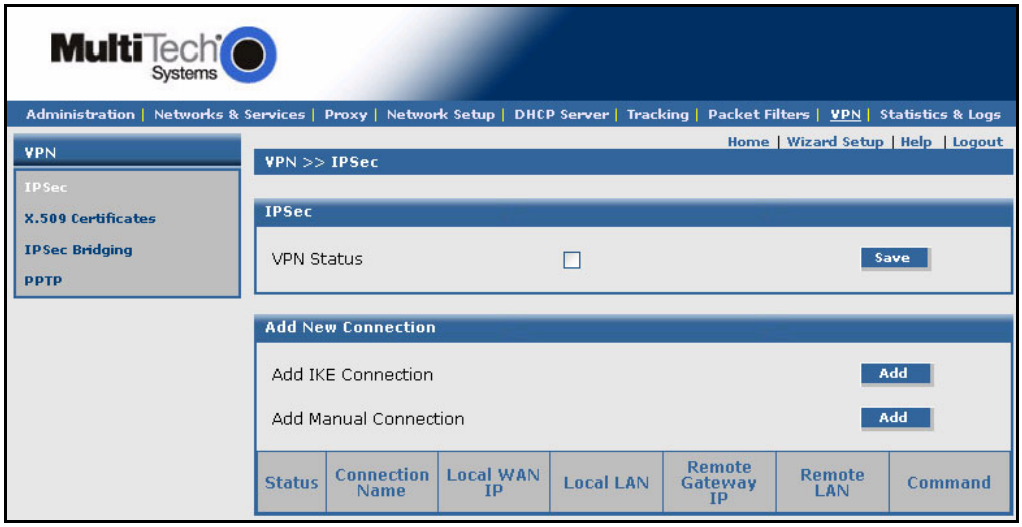


Set VPN IPSec Protocol

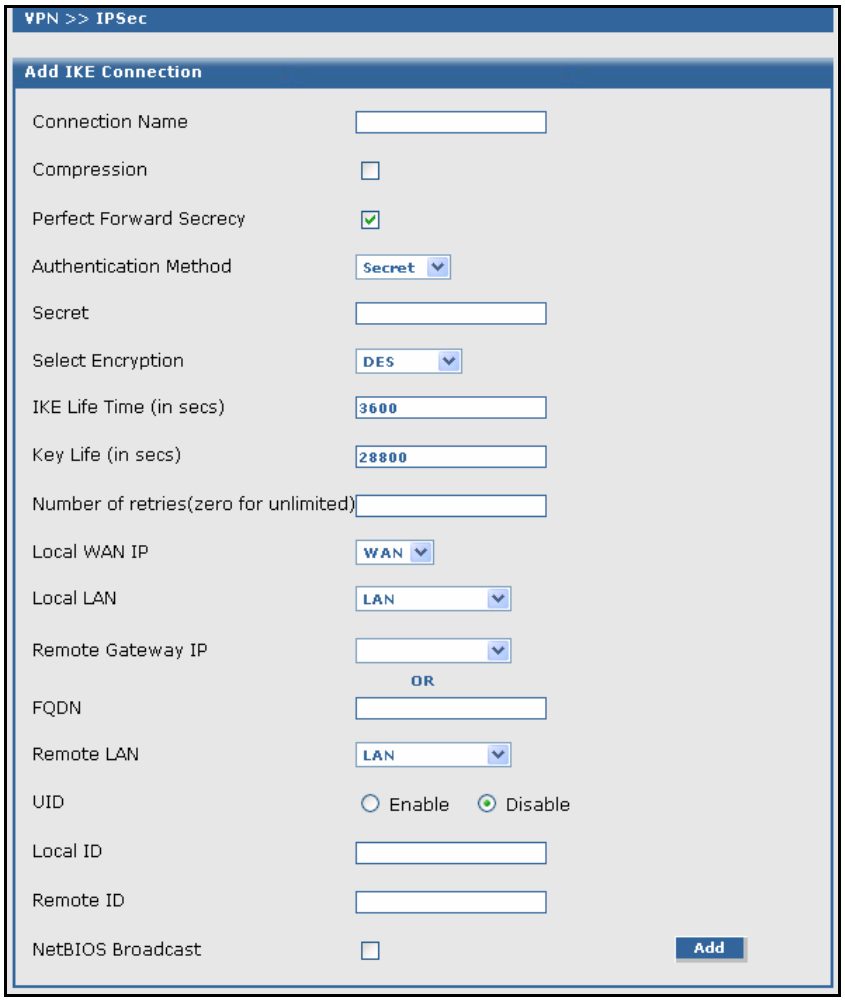
Site A Configuration: RouteFinder VPN in the Home Office

Establish an IPSec Protocol for your remote branch office access: click on **VPN > IPSec**.

1. Check the **VPN Status** box, and then click **Save**.
2. Click the **Add** button for **Add IKE Connection**.

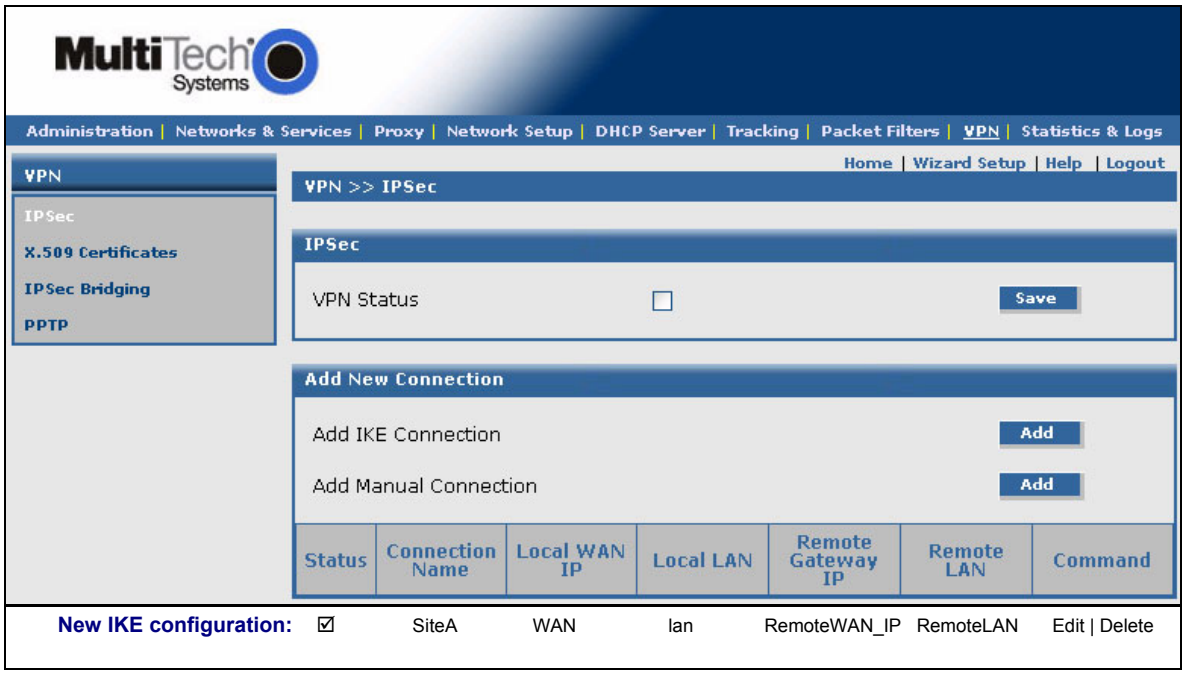


The **VPN IPSec > IKE** screen displays.



3. Enter the following information in order to establish an IPSec protocol.
   - Enter a **Connection name**. (Example: SiteA)
   - Place a checkmark in the box to enable **Perfect Forward Secrecy**.
   - Select **Secret** for the **Authentication Method**.
   - Enter a shared **Secret** string using alphanumeric characters. (Example: 1o2t3t4f)
   - Select **3DES** for **Select Encryption**.
   - Accept the defaults for **IKE Life Time** and **Key Life**.
   - Enter the number of retries you want the device to make in order to establish the connection. Use zero for unlimited retries.
   - Select the **Local WAN IP** and **Local LAN**. The Local WAN IP is the Public Static IP address of the WAN port (Example: WAN). The Local LAN is the private IP Network on the LAN port. (Example: LAN).
   - Select the **Remote Gateway IP** and **Remote LAN**. The Remote Gateway IP is the Public Static IP address of the WAN port at the Remote site (Example: RemoteWAN_IP). The Remote LAN is the private IP network on the LAN Port of the remote site (Example: RemoteLAN). Leave the Remote LAN blank.
   - Disable **UID**.
4. Click **Add**.
5. The newly created IPSec IKE configuration displays at the bottom of the **VPN > IPSec** screen. To enable the connection, check the connection's **Status** box at the bottom of the screen.

   Note: Be sure that the checkmark is still in the VPN Status box at the top of the screen. Both status boxes must be checked in order for the tunnel to start.



This completes the configuration for Site A (the RouteFinder in your home office) to support a tunnel through the Internet to remote branch office.

Configuring Site B

For Site B (RouteFinder in the branch office), input the parameters listed in the table at the beginning of this section. Then follow the steps for Site A, except that now you will use the parameters for Site B listed in the example on the first page of this chapter.

Example 2 – Remote Client-to-LAN VPN Configuration

This example shows the setup for the RF660VPN that will allow a remote client to see a LAN and where the remote client is using SSH Sentinel.

Use the VPN function to set up your RouteFinder VPN so that your network allows a remote client to have access to the LAN through a secure tunnel on the Internet. Your RouteFinder VPN includes an easy-to-use IPSec-VPN-client connection that transparently secures your Internet communications anytime, anywhere.

This setup requires:

- One RouteFinder VPN at the home office and
- A remote client with SSH Sentinel software.

For the SSH Sentinel Client Setup at the remote site, see the separate SSH Sentinel Guide.

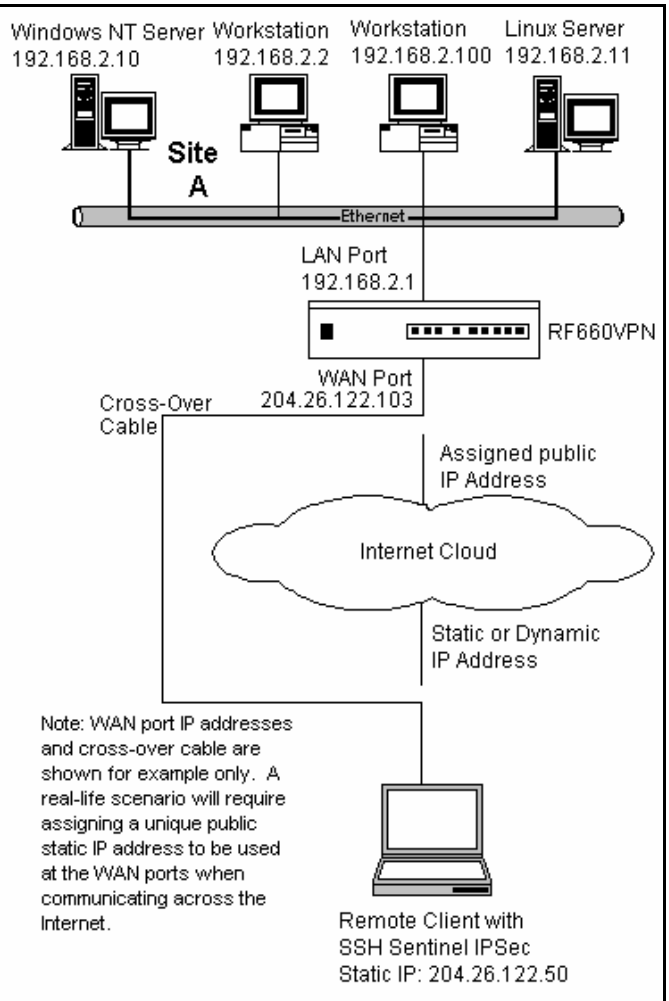
SSH Sentinel Client Accessing LAN Through RF660VPN (Input these parameters on the RF660VPN located in the home office).

1. Domain name = Sentinel
2. Public Class C = 204.26.122.x
3. Networks & Services > Network
   LAN: 192.168.2.0 – 255.255.255.0
   Sentinel_Client: 204.26.122.50 – 255.255.255.255
4. Network Setup > Interface
   Default gateway = 204.26.122.1
   Host name = RF660VPN.Site-A.com
   Eth0 = LAN, 192,168.2.1, 255.255.255.0
   Eth1 = WAN, 204.26.122.103, 255.255.255.0
   Eth2 = DMZ (don't care)

5a. Packet Filters > Packet Filter Rules (remote client static IP)
   LAN – ANY – ANY – Accept
   Sentinel – ANY – ANY – Accept

5b. Packet Filter > Packet Filter Rules (remote client dynamic IP)
   ANY – ANY – ANY – Accept

6. VPN > IPSec
   Checkmark and Save VPN Status
   Add an IKE connection:
   Connection name = Sentinel
   Checkmark Perfect Forward Secrecy
   Authentication Method = Secret
   Enter secret key (must be same both sides)
   Select Encryption = 3DES
   Local Interface = WAN
   Local LAN Subnet = LAN
   Remote IP = Sentinel_Client (remote client static IP)
   Remote IP = Any (remote client dynamic IP)
   Remote Subnet = None
   UID = Disable



Example 3 – Remote Client-to-LAN Configuration Using DNAT and Aliasing

Use this procedure to configure the RF660VPN with DNAT and Aliasing. This configuration allows a Windows 2000 Remote Client to Telnet through the RouteFinder VPN to several Windows 2000 Systems located on the LAN.

Remote Client-to-LAN Configuration Using DNAT and Aliasing Through RF660VPN

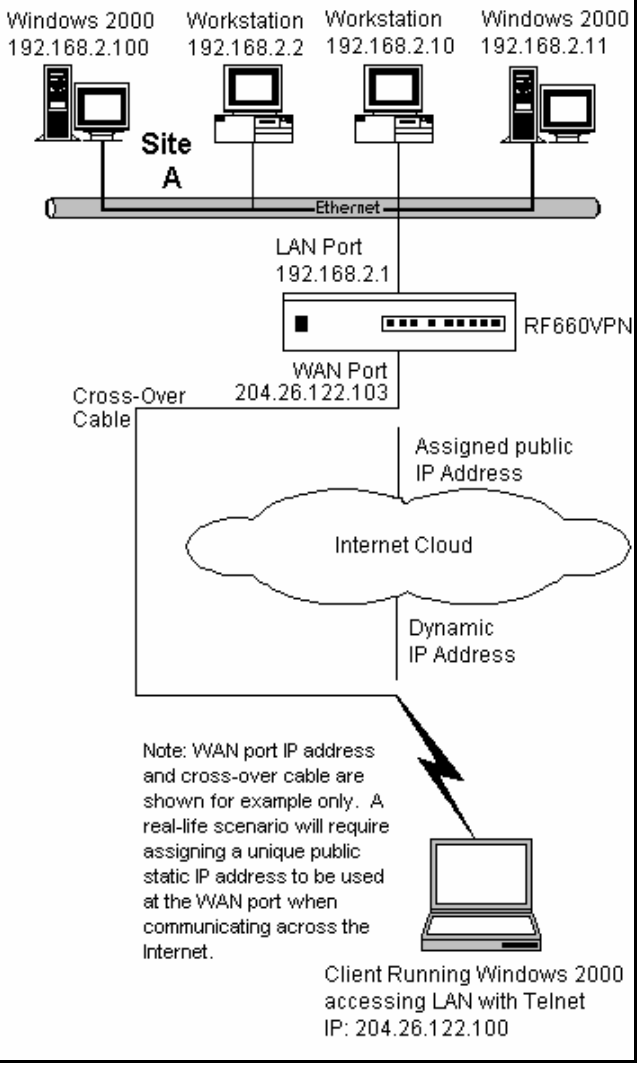
1. Networks & Services | Networks
   LAN - 192.168.2.0 - 255.255.255.0
   WANInterface - 204.26.122.103 - 255.255.255.255
   WANInterface1 - 204.26.122.104 - 255.255.255.255
   WANInterface2 - 204.26.122.105 - 255.255.255.255
   Win2k_Pro - 192.168.2.100 - 255.255.255.255
   Win2k_Server - 192.168.2.11 - 255.255.255.255

2. Network Setup | Interface
   Default gateway = 204.26.122.1
   Host name = RF660VPN.site-A.com
   eth0 = LAN, 192.168.2.1, 255.255.255.0
   eth1 = WAN, 204.26.122.103, 255.255.255.0
   eth2 = DMZ (don't care)

3. Network Setup | Interface | IP Aliases
   Eth1:0:204.26.122.104 - 255.255.255.255
   Eth1:1:204.26.122.105 - 255.255.255.255

4. Network Setup | DNAT
   WANInterface1 - Telnet - Win2k_Pro - Telnet
   WANInterface2 - Telnet - Win2k_Server - Telnet

5. Packet Filters | Packet Filter Rules
   LAN - Any - Any - ACCEPT
   Any - Telnet - Win2k_Pro - ACCEPT
   Any - Telnet - Win2k_Server - ACCEPT



Example 4 – Client-to-LAN Configuration Using PPTP Tunneling

Use this procedure to configure the RouteFinder VPN as a PPTP server for VPN Remote Client Access (aka, PPTP Roadwarrior configuration).
Note: IPX and Netbeui are not supported when using PPTP tunneling.

Remote Windows 2000 Client-to-LAN Configuration Using PPTP Tunneling Through RF660VPN

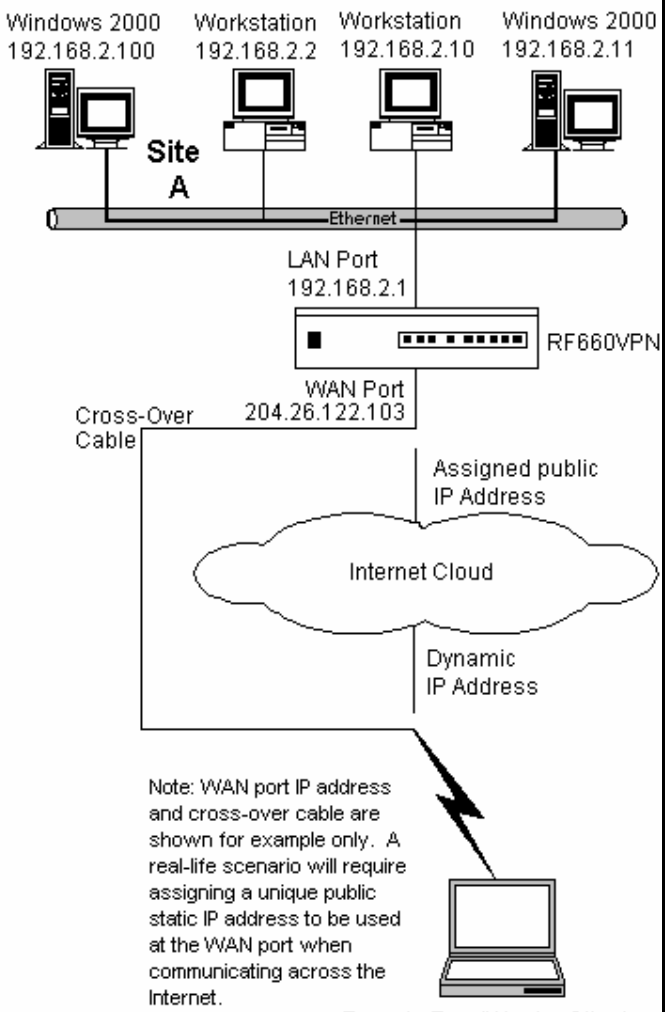
1. Networks & Services | Networks
   LAN - 192.168.2.0 - 255.255.255.0
   PPTP-Pool - 192.168.2.240 - 255.255.255.240
   (14 usable addresses)

2. Network Setup | Interface
   Default gateway = 204.26.122.1
   Host name = RF660VPN.site-A.com
   eth0 = LAN, 192.168.2.1, 255.255.255.0
   eth1 = WAN, 204.26.122.103, 255.255.255.0
   eth2 = DMZ (don't care)

3. Packet Filters | Packet Filter Rules
   LAN - Any - Any - ACCEPT

4. VPN | PPTP
   Enable PPTP Status

   Select 40 bits or 128 bits encryption strength
   Select PPTP-Pool as the remote address
   Authentication Type: Local
   Add username (roadwarrior) and password (1o2t3t4f)



Chapter 5 – URL Categorization

The Universal Resource Locator (URL) Categorization License Key allows you to set up a URL database that limits clients' access to places on the Internet by blocking sites you do not want accessed. In other words, you can deny users access to various categories of Web sites you select.

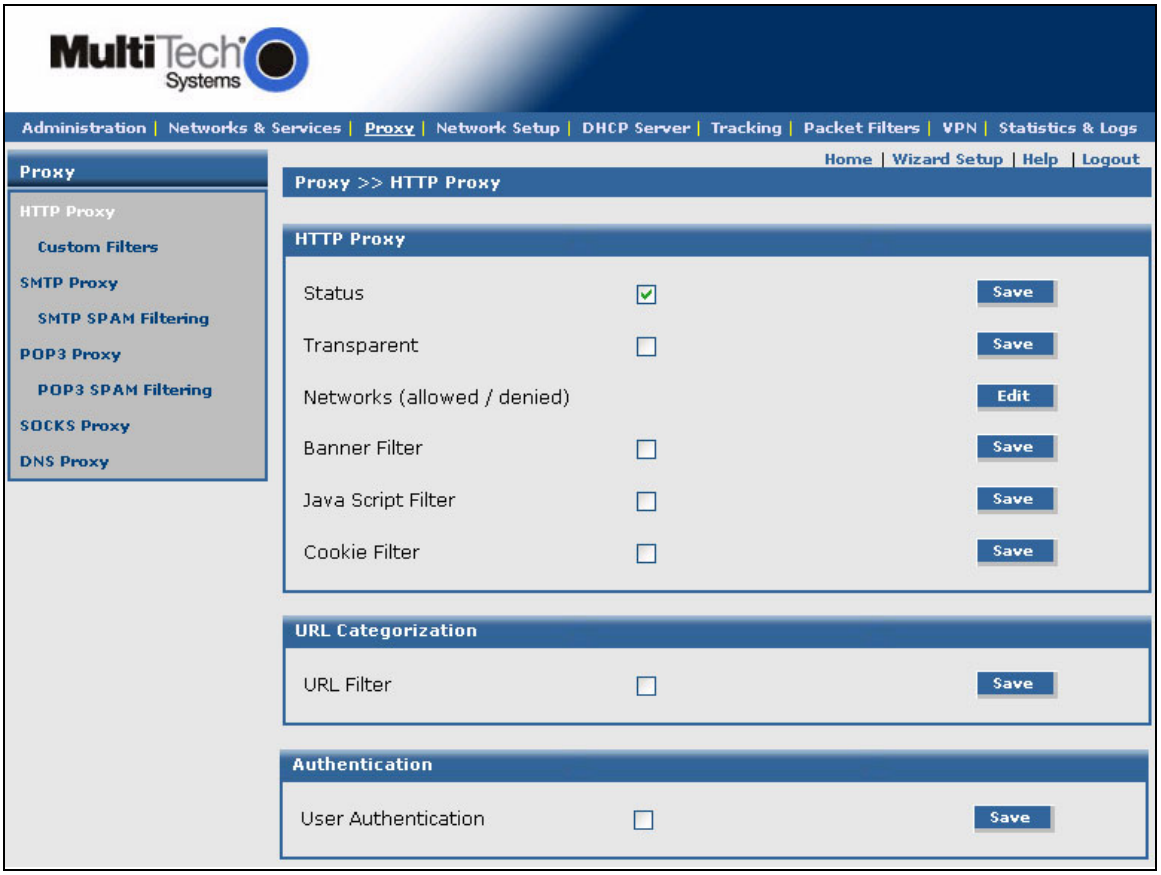
Important Settings

- Client access to the Internet works in conjunction with the HTTP proxy running in **transparent mode**.
- The RouteFinder must be connected to the Internet for the URL License to be activated.

Setting Up HTTP Proxy and URL Filtering

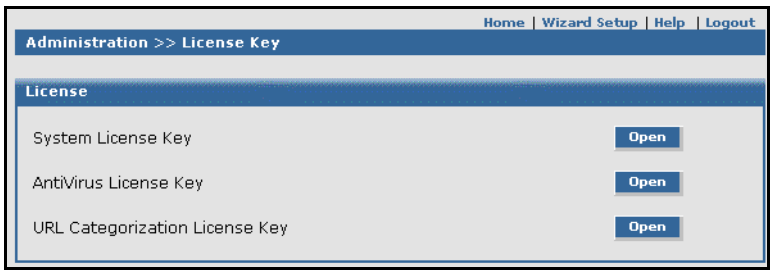
1. Click **Proxy** from the Menu bar. The **HTTP Proxy** screen displays.
2. Check the **Status** box and click **Save**.

   Important: Status must be checked before you can enter and activate your URL Categorization License Key.

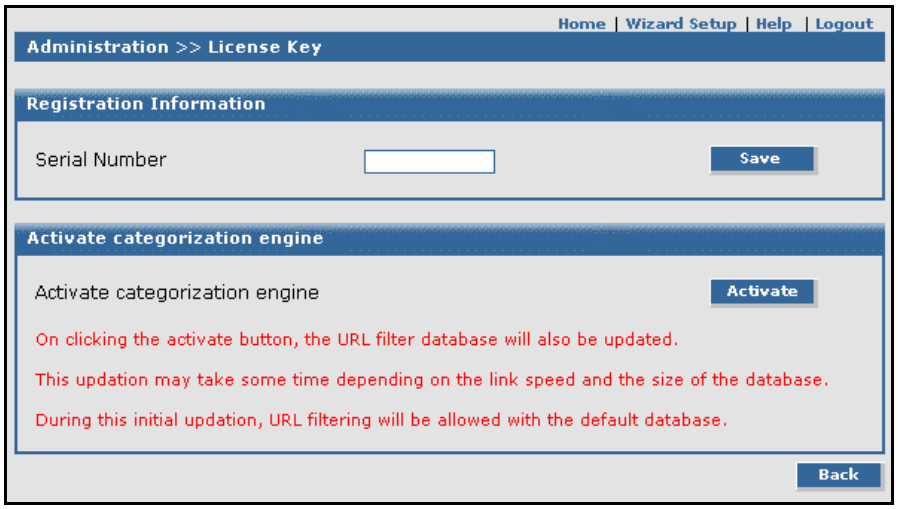


Note About URL License Key: The URL License number must be entered on the **Administration > License Key** screen before the URL Categorization section of this screen displays. The key number is located on the bottom of the RouteFinder chassis and on the front of the Quick Start Guide.

3. Enter your URL License Key.
   - Go to **Administration > License Key**.
   - Click the **Open** button for the **URL Categorization License Key**.



The **Administration > License Key > URL Categorization** screen displays. This screen shows that a license number has been entered previously. If no license has been entered, there will be a text box in which to enter the number.

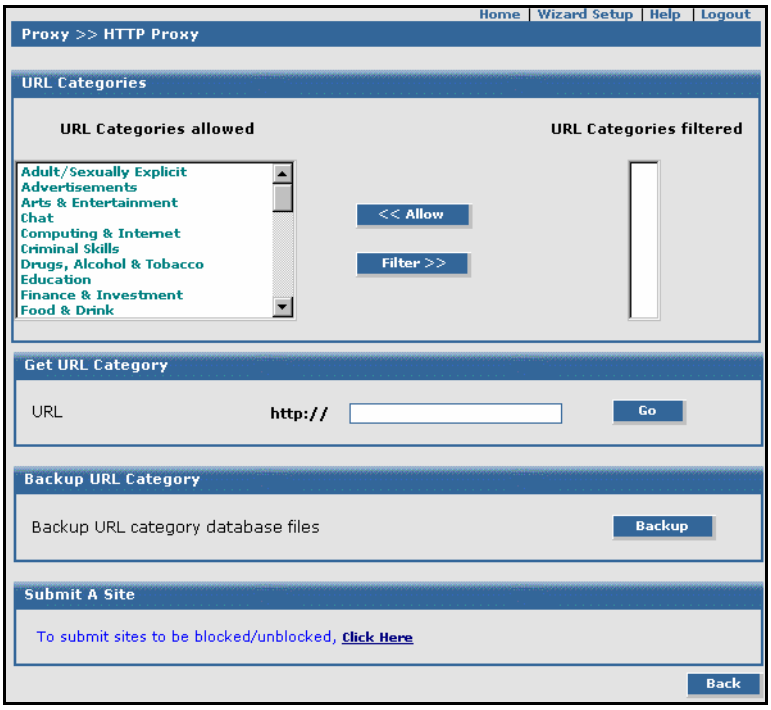

Home | Wizard Setup | Help | Logout
Administration >> License Key
Registration Information
Serial Number
Save
Activate categorization engine
Activate categorization engine
Activate
On clicking the activate button, the URL filter database will also be updated.
This updation may take some time depending on the link speed and the size of the database.
During this initial updation, URL filtering will be allowed with the default database.
Back

IMPORTANT: It is important that the serial number be entered in upper case.

- Using upper case letters, enter the 11-digit serial number of the URL License Key and click the **Save** button.
- Click the **Activate** button. The categorization engine's expiration date and time display.

4. Return to the **Proxy > HTTP Proxy** screen. See the screen on the previous page.
   - Check the **Transparent** box and click **Save**.
   - Check the **URL Filter** box and click **Save**.
   - Click **Edit** for URL Categories (Allowed/Filtered). Not shown on the screen above.

5. The **URL Categories** screen displays. You can use this screen to allow or block Web sites from users.



- Use the **Allow** and **Filter** buttons to move a URL Category from the *URL Categories Allowed* list to the *URL Categories Filtered* or from *Filtered* to *Allowed*.
- When you have established your filtered and allowed categories, click the **Backup** button to create a backup of your URL category database files.
- When you are finished organizing the categories, click the **Back** button to exit the screen.

How to Test Web Sites for Blocking

You can test specific Web sites to see if the URL has been blocked (use **Get URL Category** to perform this test) or submit a site to be blocked or unblocked by the SurfControl software, which sets up the categories stored in this software.

How to Test the Filtering

Type a URL in the **http://** box and click the **Go** button. This will test the URL to see if it is allowed or blocked.

Note: You can also test a site through your browser by entering a Web address that you feel should be blocked by the filter through one of the categories you had chosen or a category preset by the URL software. For instance, if you selected the **Finance and Investment** category to be filtered, try to access www.etrade.com. This site should be blocked. A message displays under the URL address stating the status of this Web site.

Important: The sites listed in the **Favorites** box of the browser will not be blocked unless the cache is emptied in the browser.

Establishing Filtering Rules for Networks and Hosts

Return to the **Proxy > HTTP Proxy** screen by clicking the **Back** button on the **Proxy > HTTP Proxy > URL Categorization** screen.

- Click the **Edit** button for **Networks / Hosts to bypass URL Filtering**. The **Networks / Hosts to bypass URL Filtering** screen displays. You can use this screen to allow or block Web sites from Networks / Hosts.
- Click the **Add** button to move a network/host name into the **Network/Hosts to Bypass URL Filtering** box.
- If you decide you do not want one or more of the networks/hosts bypassing the filter, select the name and click the **Delete** button. The name moves back into the **Available Networks/Host** box.

Submitting a Site to SurfControl for Reconsideration

Filter categories are setup and controlled by the *SurfControl* software that is built into your RouteFinder VPN. There may be a category you would like to see added or deleted. The User Guide provides instructions for these requests.

MultiTech®
Systems